

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

United States of America,
Plaintiff,

v.

Michael James McCutchin,
Defendant.

No. CR-17-01517-001-TUC-JAS (BPV)

ORDER

Pending before the Court is a Report and Recommendation issued by Magistrate Judge Bernardo P. Velasco. (Doc. 71.) In the Report and Recommendation, Magistrate Judge Velasco recommends that the Court deny Defendant's Motion to Suppress (Doc. 35). As the Court finds that the Report and Recommendation appropriately resolved the Defendant's Motion to Suppress (Doc. 35), the objections are denied.¹ However, the Court will expand on its reasoning.

FACTS²

On July 24, 2016, the Department of Homeland Security Special Agent (SA) Robert McCarthy identified an Internet Protocol (IP) address that he previously accessed child pornography through a peer-to-peer file-sharing network. SA McCarthy identified that the

¹ The Court reviews de novo the objected-to portions of the Report and Recommendation. 28 U.S.C. § 636(b)(1); Fed. R. Crim. P. 59(b). The Court reviews for clear error the unobjected-to portions of the Report and Recommendation. *See Johnson v. Zema Systems Corp.*, 170 F.3d 734, 739 (7th Cir. 1999); *see also Conley v. Crabtree*, 14 F. Supp. 2d 1203, 1204 (D. Or. 1998).

² The facts from the Report and Recommendation are adopted as the Court does not find that they are clearly erroneous. The Court supplemented facts from the parties' briefing or the witnesses before the Magistrate Judge.

1 IP address belonged to Cox Communications, which would then lease the IP address to its
2 consumers. On August 26, 2016, the Department served a Summons under 19 U.S.C.
3 § 1509 on Cox Communications, requiring that it provide customer/subscriber information
4 attached to the previously-identified IP address during the time that SA McCarthy
5 connected it to child pornography. Cox Communications returned the account information
6 for John McCutchin. John McCutchin is Defendant's father. The residential address
7 attached to the Cox Communications account was owned by John McCutchin. John
8 McCutchin resided there with his son and brother-in-law,³ who resides at the address part
9 time. All the residents report connecting devices to and utilizing the internet under John
10 McCutchin's account and therefore all the residents utilized the IP address in question.

11 After further investigation, SA McCarthy applied for a search warrant. On
12 November 22, 2016, Magistrate Judge Lynette Kimmins signed the search warrant for
13 Defendant's home. During the execution of the warrant, agents questioned Defendant and
14 his father; the brother-in-law was not present during the search. Agents seized several
15 electronic devices. Subsequent forensic examination of the devices uncovered child
16 pornography on Defendant's devices.

17 The grand jury returned a six-count indictment against Defendant in this matter.
18 Defendant filed a motion to suppress (Doc. 35). The Government responded (Doc. 54) and
19 filed a notice of supplemental authority (Doc. 59). Defendant filed his reply (Doc. 60). On
20 October 30, 2018, Magistrate Judge Velasco held an evidentiary hearing on the matter
21 (Doc. 62). Defendant requested that the parties be permitted to file their closing arguments
22 in the form of written briefs. On December 12, 2018, Defendant filed his Memorandum in
23 Support of His Motion to Suppress (Doc. 66). On December 26, 2018, Government
24 responded to Defendant's memorandum (Doc. 69). On February 1, 2019, Magistrate Judge
25 Velasco filed his Report and Recommendation recommending that the Court deny
26 Defendant's motion (Doc. 71). Defendant timely objected (Doc. 75) and the Government

27
28 ³ The Magistrate Judge identified this individual as a son-in-law. The Court believes this
is an error as the testimony identifies him as John McCutchin's brother-in-law. However,
this error does not affect the Magistrate Judge's analysis.

1 timely responded (Doc. 78).

2 ANALYSIS

3 The Defendant presents several arguments to the Court in the Motion to Suppress
4 and the subsequent briefing. (Docs. 35, 60, 66.) First, Defendant argues that the summons
5 presented to Cox Communications violated the statutory limits of 19 U.S.C. § 1509.⁴ (Doc.
6 35 at 5.) The Government rejects this notion and argues that the alleged statutory violation
7 would not provide for exclusion of the resulting evidence. (Doc. 54 at 9–10.) Exclusion is
8 “‘primarily to deter constitutional violations’ and violations of statutes that enforce
9 constitutional norms.” *United States v. Dreyer*, 804 F.3d 1266, 1278 (9th Cir. 2015)
10 (internal citation omitted). The exclusionary rule is rarely used to remedy statutory
11 violations. *Id.* at 1278–79; *United States v. Lombera-Camorlinga*, 206 F.3d 882, 886–87
12 (9th Cir. 2000). The Court has not found, and Defendant has not presented, any indication
13 that violation of 19 U.S.C. § 1509 is one of the rare instances when exclusion would be
14 appropriate absent a constitutional violation. Therefore, the Court will not decide if § 1509
15 was the appropriate method to request subscriber information, but instead determine if
16 Defendant or his father had a Fourth Amendment privacy interest in his father’s subscriber
17 information.

18 Defendant argues that there is a privacy interest in the subscriber information after
19 *Carpenter v. United States*, 138 S. Ct. 2206 (2018). (Doc. 35 at 6–10.) The Government
20 rejects this argument and challenge Defendant’s standing to present this matter. (Doc. 54
21 at 4–9.) The Court may address Fourth Amendment standing after addressing the merits of
22 the claim, if necessary. *Byrd v. United States*, 138 S. Ct. 1518, 1530 (2018). In *Carpenter*,
23 the government obtained location points known as cell-site location information (CSLI)
24 from the defendant’s two cellphone providers. 138 S. Ct. at 2212. The government did not

25
26 ⁴ During this argument, Defendant cited to *United States v. Ackerman*, 831 F.3d 1292 (10th
27 Cir. 2016) for the proposition that digital images are chattel. (Doc. 35 at 5.) It is unclear if
28 Defendant is attempting to present a trespass argument under *United States v. Jones*, 565
U.S. 400 (2012). The Court will not consider this argument as the alleged “trespass” in this
matter was not of the pictures as in *Ackerman* but was instead of the subscriber information
records, which is more appropriately considered under a reasonable-expectation-of-privacy
analysis. *See* 831 F.3d at 1294–95.

1 apply for or receive a warrant for the information. *Id.* The Supreme Court of the United
2 States acknowledged the changing technological advances, particularly with respect to a
3 cellphone’s ability to store vast amounts of extremely sensitive information that is
4 “detailed, encyclopedic, and effortlessly compiled.” *Id.* at 2214, 2216. The Supreme Court
5 distinguished *Carpenter* from the previous third-party doctrine cases due to the “unique
6 nature of cell phone location records.” *Id.* at 2217. The records “reveal[] not only [a
7 person’s] particular movements, but through them [the person’s] ‘familial, political,
8 professional, religious, and sexual associations.’” *Id.* (internal citation omitted). After the
9 Court “decline[d] to extend *Smith* and *Miller* to the collection of CSLI,” the Court took
10 care to keep the third-party doctrine cases intact. *Id.* at 2220 (“Our decision today is a
11 narrow one. . . . We do not disturb the application of *Smith* and *Miller* or call into question
12 conventional surveillance techniques and tools, such as security cameras. Nor do we
13 address other business records that might incidentally reveal location information.”). The
14 internet subscriber information differs drastically from the CSLI obtained in *Carpenter*. It
15 provides business records that are not detailed or encyclopedic. Subscriber information
16 does not reveal familial, political, professional, religious, sexual associations, or location.
17 The Court finds that neither Defendant or John McCutchin has a reasonable expectation of
18 privacy to the internet subscriber information as it fits squarely within the third-party
19 doctrine. *See United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018).

20 Defendant argues that Defendant had a privacy interest in the IP address. (Doc. 35
21 at 13.) This argument is presented without any law, or facts as to how SA McCarthy
22 obtained the IP address in this matter. (*Id.*) The Court finds that this argument fails on its
23 merits for the same reason that the subscriber information argument fails. The IP address
24 is much like a return address on an envelope or a phone number; it is the IP address that is
25 relayed to websites and allows the requested website to send information to a computer.
26 (Doc. 70 at 14.) There is no doubt that a person does not have a privacy interest in what is
27 put out publicly into the world, such as a return address on an envelope or phone number
28 dialed. *United States v. Choate*, 576 F.2d 165, 174–78 (9th Cir. 1978) (finding that the

1 gathering of address information from envelopes, not content within the envelopes, is not
2 a Fourth Amendment search); *see Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)
3 (considering the privacy expectations of phone numbers dialed out of a private residence
4 and finding that there is no legitimate expectation of privacy in the numbers dialed).
5 Defendant seems to argue that people could do nefarious things with an IP address. (Doc.
6 70 at 21–23.) Defendant never follows that assertion with law, stating that if a piece of
7 information could be used for nefarious purposes there is an increased privacy interest.
8 (Docs. 35, 60, 66, 75.) A return address on an envelope could be used by burglars or identity
9 thieves, bank records could be useful to hackers or identity thieves, and location data may
10 be useful to similar groups, but the ability for people to do nefarious things with the
11 information is not a part of the Fourth Amendment analysis. *Carpenter*, 138 S. Ct. at 2217–
12 20 (not considering potential for location data to be used nefariously when discussing the
13 defendant’s reasonable expectation of privacy); *Smith*, 442 U.S. at 743–44; *United States*
14 *v. Miller*, 425 U.S. 435, 442–43 (1976); *Choate*, 576 F.2d at 174–75. The Court finds that
15 Defendant does not have a privacy interest in the IP address used to connect his home with
16 the internet.

17 Defendant argues that the search warrant used to search the home was a “general
18 warrant” and violated his Fourth Amendment rights because the warrant was based on stale
19 information and not on probable cause. (Doc. 35 at 11–12.) The Government argues that
20 this was not a general warrant and instead it was supported by probable cause to search
21 devices able to access the internet to distribute or obtain child pornography. (Doc. 54 at
22 11–14.) The Court shall review the warrant with great deference for the issuing judge.
23 *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (quoting *Spinelli v. United States*, 393 U.S. 410,
24 419 (1969)). The Fourth Amendment requires that warrants are based on probable cause
25 supported by oath and describe with particularity the place to be searched and items to be
26 seized. U.S. Const. amend. IV; *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir.
27 2006) (en banc).

28 There is probable cause if is “there is a fair probability that contraband or evidence

1 of a crime will be found in a particular place.” *Gates*, 462 U.S. at 214. When courts find
2 that search warrants include illegally obtained information, it should purge the offending
3 information and determine the sufficiency with the remaining information. *United States*
4 *v. Bishop*, 264 F.3d 919, 924 (9th Cir. 2001) (internal citation omitted). The Court has
5 found that the IP address and subscriber information were legally gathered or not
6 appropriate for suppression and therefore it is not appropriate to purge any information in
7 the contested search warrant. *See id.* The evidence obtained in July 2016 regarding
8 Defendant’s IP address downloading pornographic material depicting minors was not stale
9 in November 2016. *United States v. Flores*, 802 F.3d 1028, 1044 (9th Cir. 2015) (finding
10 that passage of time is not the controlling question when analyzing staleness, particularly
11 with electronic evidence, of information collected more than three months prior to the
12 warrant) (quoting *Gourde*, 440 F.3d at 1071); *United States v. Schesso*, 730 F.3d 1040,
13 1042 (9th Cir. 2013) (holding that a twenty month delay between suspected download of
14 illegal electronic material and the execution of the warrant did not render the information
15 stale). Defendant argues that there is no belief that any particular computer or device
16 accessed child pornography. (Doc. 35 at 12.) Probable cause is satisfied if there was a
17 probability that evidence or contraband would be found in a particular place; in this matter,
18 there was a probability that child pornography would be found on an electronic device in
19 Defendant’s home as the unique IP address for Defendant’s home was connected with the
20 possession of child pornography. *See Schesso*, 730 F.3d at 1046 (finding probable cause
21 when the IP address connected to defendant’s home was connected with a child
22 pornography video on a peer-to-peer file-sharing network twenty months prior); *United*
23 *States v. Nguyen*, 743 F. App’x 764, 766 (9th Cir. 2018) (mem.) (finding that child
24 pornography being shared from a computer using a certain IP address was sufficient
25 probable cause that evidence of a crime would be found in defendant’s home). The Court
26 finds that the warrant in this matter was supported by probable cause and is not a general
27 warrant.

28 The Government also presents a good faith argument. (Doc. 54 at 15–16.) The Court

1 does not reach a conclusion on this matter, as Defendant's arguments fail on the merits.

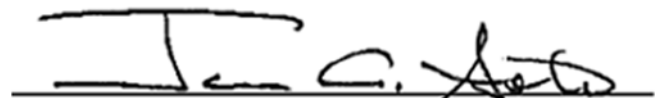
2 **CONCLUSION**

3 Accordingly, IT IS HEREBY ORDERED as follows:

4 (1) Magistrate Judge Velasco's Report and Recommendation (Doc. 71) is accepted and
5 adopted.

6 (2) Defendant's Motion to Suppress (Doc. 35) is denied.

7 Dated this 7th day of March, 2019.

8
9
10 

11 Honorable James A. Soto
12 United States District Judge
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28